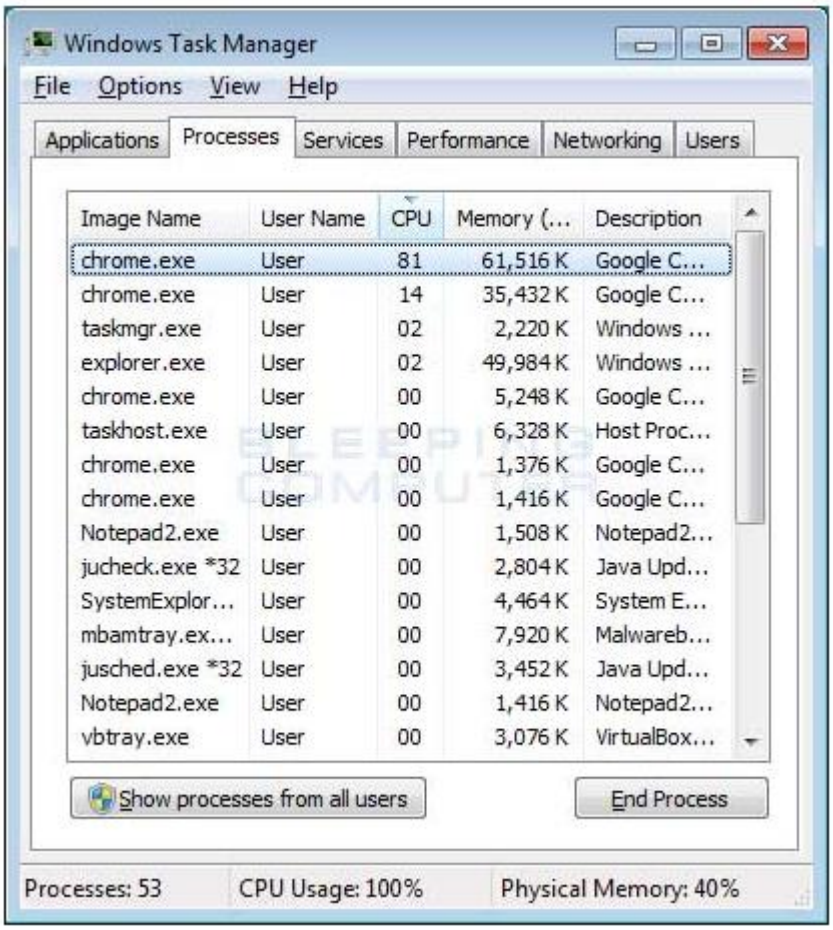
National Datacenter

Таны интернет хөтчийг ашиглан цахим валют олборлож буйг илрүүлэх

Интернет хөтөч ашиглан цахим валют олборлодог болсон нь маш том асуудлуудыг дагуулж байна. Интернет хөтчид олборлолт хийдэг “CoinHive” гэх скрипт болон “Web extension” нь маш олон цахим хуудсыг халдварлуулж олон тооны хэрэглэгчид энэ халдлагад өртсөөр байна. Энэхүү халдлагад интернет хөтөч өртсөнөөр “Monero” гэх цахим валют олборлох ба энэ нь таны комьпютерийн “CPU”-г дээд хүчин чадлаар нь ажиллуулж халаах ба их халсны улмаас “CPU” гэмтэж эвдрэх эрсдэлтэй болдог ажээ.

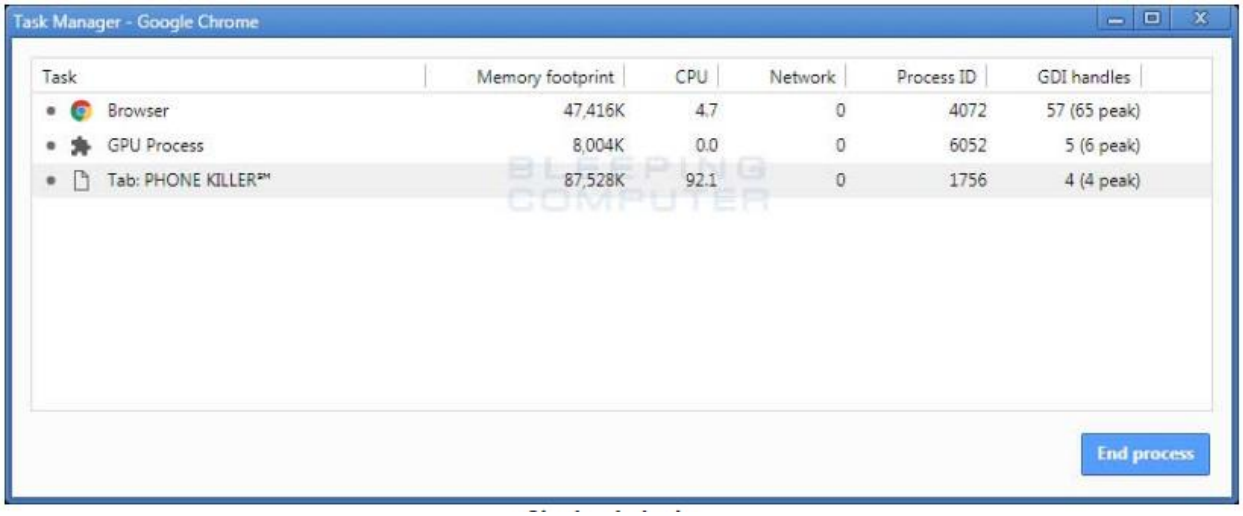


“Chrome” нь “CPU”-нд их ачаалал өгч байгааг харуулж байгаа боловч яг юунаас болж ачаалал ихэссэнийг тодорхой харуулдаггүй. “Chrome”-ын “task manager” дээрээс таны интернет хөтөч цахим валют олборлож байгаа эсэхийг мэдэх боломжтой.

“CPU”-нд ачаалал өгч буй цахим хуудсуудыг илрүүлэх

Хэрэв интернет хөтөч “Chrome” нь “CPU”-г хэт их ачааллаж байвал тухайн цахим хуудас болон өргөтгөлийг тодорхойлох хэрэгтэй. Та “Chrome” дээрээ “Shift+ESC” гарын хослолыг дарах эсвэл “menu” товчин дээр даран “More tools+Task manager”-ыг сонгож ажиллуулах хэрэгтэй.

“Chrome Task manager”-г ажиллуулахад “Chrome” дээр ажиллаж байгаа процессуудын жагсаалт болон “CPU”-ны ашиглалтыг харах болно.

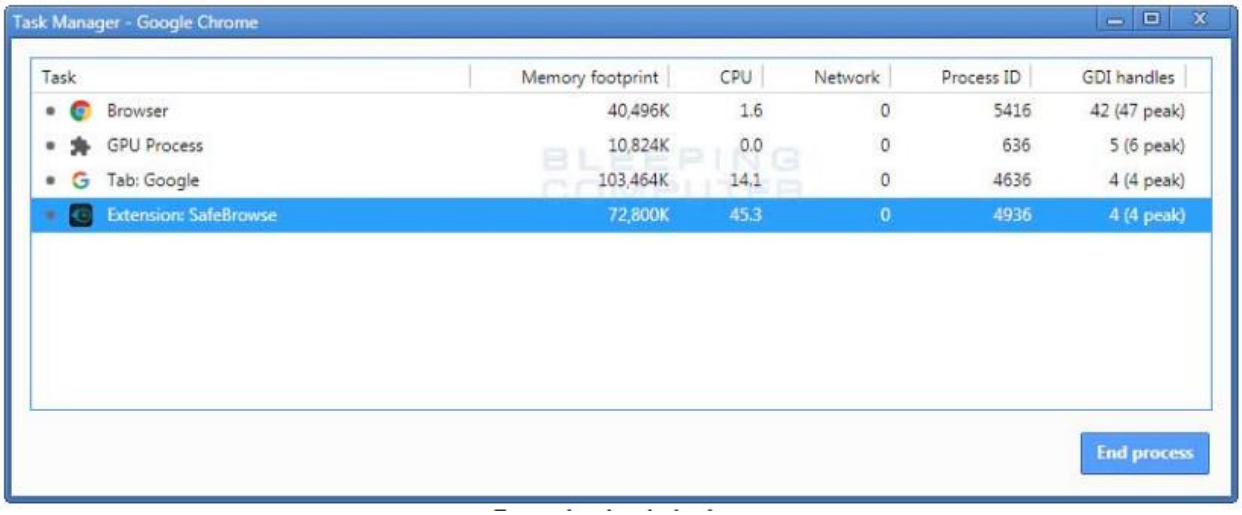


Дээрх зураг дээр “PHONE KILLER” процесс нь “CPU”-ны 92%-ыг ашиглаж байна. Энэхүү ачааллаж байгаа процессыг зогсоохын тулд та тухайн “PHONE KILLER” процессыг

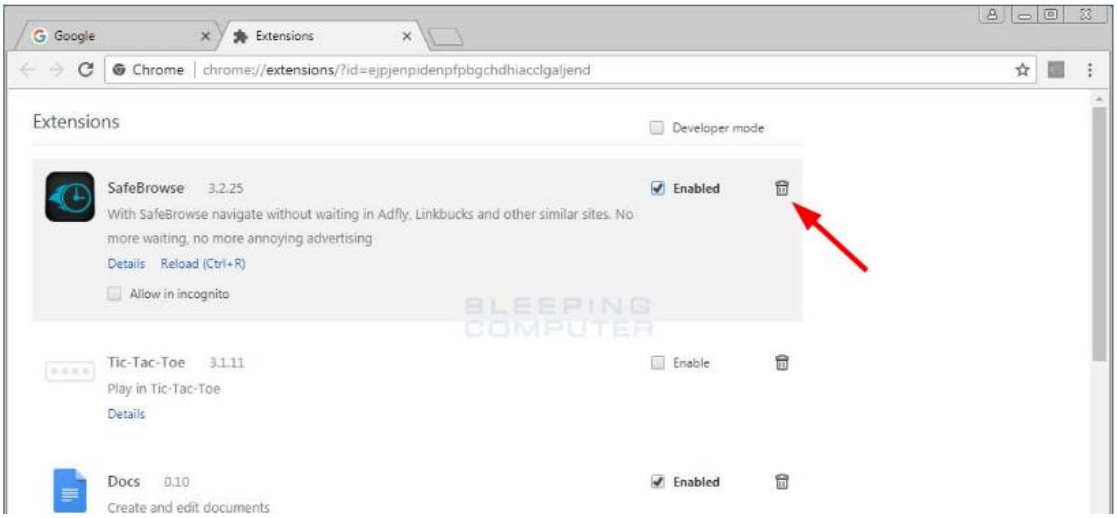
сонгоод “End process” дээр дарах хэрэгтэй. Процессыг зогсоосны дараа таны компьютер хэвийн ажиллаж эхлэх бөгөөд тухайн процессыг ажиллуулж буй цахим хуудас -руу дахин орохгүй байхыг анхааруулъя.

Цахим валют олборлож нэмэлтүүдийг (extensions) илрүүлэх

Зөвхөн цахим хуудас нь “CPU”-г ачааллахгүй бөгөөд нэмэлтүүд (extensions) нь мөн өндөр ачаалал үзүүлдэг. Интернет хөтчид олборлолт хийдэг “CoinHive” гэх скрипт нь “SafeBrowse” гэх нэмэлтийг суулгаснаар ажилдаг байна. “Chrome Task manager” дээрээс тухайн нэмэлт (extension) нь маш олон процесс ажиллуулж байгаа нь харагдана.



Ачааллаж буй нэмэлт дээр дархад “chrome” дээр ажиллаж буй нэмэлтүүдийн жагсаалт руу орох бөгөөд хогийн сав дээр даран “SafeBrowse” гэх нэмэлтийг (extension) устгаж дахин суулгахгүй байх хэрэгтэй юм.



Цахим валют олборлогчоос өөрийгөө хамгаалах

Интернет хөтөч ашиглан цахим валют олборлогч нар өдөр бүр нэмэгдсээр байна. Тиймээс хэрэглэгчид та бүхэн “CoinHive” гэх мэт скрипт-үүдийг илрүүлэх чадал бүхий вирусны эсрэг програм хангамж суулгаж шинэчлэлийг байнга хийгээрэй.

Мөн та “chrome” дээр “adblocker” гэх нэмэлтийг суулгаж цахим валют олборлогчоос хамгаалж болно. Илүү нарийн хамгаалалт хийхийг хүсвэл “https://github.com/keraf/NoCoin/blob/master/src/blacklist.txt” цахим дээрх жагсаалтаас цахим валют олборлогч нартай холбоотой цахим хуудаснууд болон “IP” хаягуудын жагсаалтыг харж хаах боломжтой.

Эх сурвалж: https://www.bleepingcomputer.com/news/security/using-the-chrome-task-manager-to-find-in-browser-miners/

2018.03.13